Combating Ransomware: A Brief Look into The Biggest Ransomware Attack

[1]Aaron Lobo, [2]Vikrant Gurav, [3]Chaitanya Tule, [4]Paritosh Kadam

[1,2,3,4]UG Student, Vidyalankar Institute of Technology, Mumbai, India,

[1]aaronnlobo11@gmail.com, [2]kv7gaming@gmail.com, [3]chaitanya.tule19@gmail.com, [4]paritosh1400@gmail.com

Abstract: With the increasing dependence on online means due to the pandemic, the need for reliable security and privacy has been more prominent than ever. Certain issues such as Ransomware have caused widespread issues in the tech world notably with the "WannaCry" Ransomware in 2017. In this paper, we discuss how Ransomware works and the threats and financial implications it poses to users. The paper also talks about the working of the "WannaCry" and the various effects it caused. Furthermore, we try to spread awareness to prevent users being vulnerable to Ransomware issues.

Keywords* — *Ransomware, CyberSecurity, Information Security, WannaCry, Cryptocurrencies, Cryptography.

I. Introduction

Due to everyone [2] being holed up inside during the pandemic, there is an ever-increasing number of cyberattacks on personal and organizational computers. This includes the likes of ransomware, which is a type of malware that encrypts all kinds of files on the machine, and the attacker then proceeds to ask the victim to pay to gain access to the files again by decrypting the data, which is usually not the case after the payment is completed. With many organizations moving into the digital era in which the world is transitioning, more data is susceptible to these attacks. Many newer organizations do not have the necessary security measures to protect their data against ransomware attacks. The motive behind ransomware attacks is primarily financial gain due to greed. The payment in these attacks is generally made through Bitcoin transfers. It is a decentralized currency which means that there is almost no identifying information for any party participating in a transfer. This effectively makes the attacker anonymous, and law enforcement cannot freeze bitcoin accounts as they would any other bank accounts. There are two major types of ransomware: Crypto-Ransomware and Locker Ransomware. Crypto Ransomware focuses on encrypting files and asking for ransom through cryptocurrencies, while Locker ransomware locks the victim out of the device until he/she makes the ransom payment.

II. How Ransomware Works

A. *Infection and Distribution*

Ransomware can be injected into organization machines in many different ways. They usually spread through worms and do not need any external factor to instigate the transfer from one device to another in a network. Phishing emails are also a way for attackers. They manipulate victims to open a link to a malicious website that downloads and executes the ransomware on the victim's machine. Attackers also use RDP or Remote Desktop Protocol to download ransomware on the victim's devices. Sometimes the infection can be done directly, like in the case of WannaCry exploiting the Eternal Blue vulnerability.

B. *Encryption*

As soon as ransomware installs on the victim's system, it encrypts all the files. All operating systems have encryption functionalities, and the attacker simply introduces an encryption key that encrypts all the original files. The ransomware, however, has to make sure to maintain the system stability and not encrypt any system-related files to ensure the working of the system.

C. *Ransom Demand*

When all files have been encrypted, the ransomware makes a ransom demand. Generally, the ransomware changes the wallpaper to a ransom note detailing the steps to be taken by the victim to recover their data without it being destroyed or deleted. The attacker usually demands a certain amount of money in the form of cryptocurrency like Bitcoin. Once the ransom is paid, the attacker provides a copy of the private key used to protect the symmetric encryption key or a copy of the symmetric encryption key itself.

III. History Of Ransomware

Since the early 2010s, [1] ransomware attacks have been increasing with the advancements in technology and more data being stored on computers rather than on paper.

Some of the significant attacks throughout the years include:

A. *1989 - AIDS Trojan/PC Cyborg*

This attack is the first known case of ransomware. It was delivered through distributed floppy disks that contained a

DOI : 10.35291/2454-9150.2022.0008

virus. This virus counted the number of times the computer booted up, and at the 90th time, it hid all directories and also encrypted filenames. Then an image that demanded users to mail $189 to a postal address in Panama showed up on the screen. However, the decryption process of this was straightforward.

B. 2012 - Reveton

Based on the Citadel Trojan, the Reveton Trojan ransomware started spreading through Europe. This ransomware claimed that the victim's computer was used for illegal activities like downloading unlicensed products or child pornography, due to which it is also called "Police Trojan". To deceive the victims further, the screen displayed the computer's IP address or footage from the victim's webcam. The victims were instructed to make a payment through a prepaid cash service like Ukash or Paysafecard.

C. 2013 - CryptoLocker

This ransomware was difficult to repair due to its very long key sizes. It was based on public-key cryptography. It generated a 2048-bit RSA key pair and stored the private key on the command and control center. It used the public key to encrypt particular files. A message was displayed stating a deadline and offering to decrypt the files if payment through bitcoin or pre-paid cash voucher was made. However, there was no guarantee of this. In May 2014, CryptoLocker isolated Operation Tovar, which took down the botnet used to distribute the malware Gameover ZeuS botnet.

D. 2014 - CryptoWall

In 2014, another generic ransomware called CryptoWall started surfacing where as usual files were encrypted by the ransomware and victims were demanded to pay to gain access to the decryption program. The attackers demanded payment in the form of prepaid cards or BitCoin. CryptoWall caused roughly $18 million in damages due to there being many different versions of the ransomware, making it difficult to trace and combat.

E. 2015 - TeslaCrypt

TeslaCrypt samples were based on an earlier program called CryptoLocker and were circulated in November 2014 but were not distributed until March of 2015. TeslaCrypt initially targeted gamers, and a popup on their computers directed them to pay a $500 ransom in bitcoin. In May 2016, the issue was resolved when the developers of TeslaCrypt released a master decryption key for affected users to get access to their computers.

F. 2016 - Locky

It was discovered in [5] 2016 this ransomware was infamous for the high number of infection attempts it made on computer networks. The attack came in the form of an email with an invoice attached from someone claiming to be a company employee. Lock's main objective was to Lock the computer files, which would force users to pay a ransom in cryptocurrency in exchange for the decryption tool, which would unlock the computer files.

G. 2017 - WannaCry

In May of 2017, a ransomware called WannaCry infected computers worldwide by exploiting a vulnerability in Windows PCs. More than 200,000 computers around the world were infected. Victims included Spanish company Telefonica and many hospitals in the UK. A total of 150 countries were affected by the attack, and the total estimated loss was around $4 billion globally. WannaCry attacks continue to this day, with attackers demanding $300 in bitcoin to unlock the infected computer systems.

H. 2020 - University of California

In June of 2020, it was reported that the UCSF School of Medicine's IT system had been exploited by a hacking team called Netwalker. The medical research institution had been working on a cure for COVID. The team demanded a $3 million ransom payment. After negotiations, the UCSF paid the bitcoin equivalent of the price to resolve the cyber attack.

I. 2020 - CWT

A US business travel management firm, CWT, disclosed that it had fallen victim to a ransomware attack that infected its systems. Using a ransomware called Ragnar Locker, the attackers stole susceptible corporate files and rendered 30,000 computers offline. The company paid the hackers about $4.5 million for the security of their data.

J. 2021 - CNA Financial

In March of 2021, CNA Financial, the seventh-largest commercial insurer in the US, reported that it had sustained a cybersecurity attack. The attack was carried out by a group called Phoenix, which used Ransomware known as Phoenix Locker. Eventually, they had to pay $40 million in May to get their data back.

K. 2021 - Brenntag

In April 2021, a German chemical distributor Brenntag reported that it was the target of a cyberattack by Darkside, which stole 150 GB of data and threatened to leak if ransom demands weren't met. After negotiating with the criminals Brenntatg ended up reducing the original ransom of $7.5 million to $4.4 million.

L. 2021 - JBS

JBS, one of the largest meat suppliers in the US, disclosed a hack that caused the company to temporarily stop its operations at 5 of its largest US-based plants. The attack also disrupted the company's Australia and UK branches. JBS had to pay the assailants $11 million ransom in Bitcoin to prevent any further disruption and reverse the impact on the grocery stores and restaurants. The FBI identified the attackers as a

DOI : 10.35291/2454-9150.2022.0008

group called REvil, a well-known criminal group specializing in ransomware attacks.

M. 2021 - Kaseya

In July of 2021, Kaseya announced that it had been attacked by a group of attackers. Kaseya is a company that provides IT solutions for other companies. Due to the attack on Kaseya, it caused a domino effect that ended up affecting more than 1500 organizations in multiple countries. REvil, the group of hackers responsible for the attack on JBS a few months ago, was the one that targeted Kaseya and was demanding ransoms ranging from a few thousand dollars to multiple millions, according to a Reuters report. REvil demanded $70 million in bitcoin from Kaseya, which they declined to pay and instead decided to cooperate with the FBI and the Cryptocurrency and Infrastructure Agency to mend the attack. On July 21, 2021, they obtained a universal decryptor key and distributed it to the organizations affected by the attack.

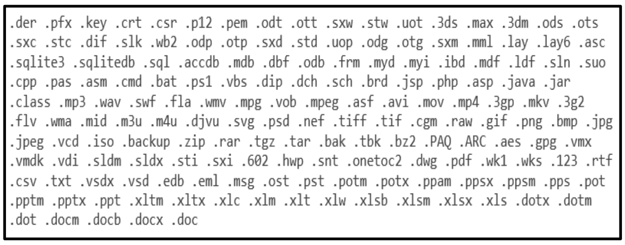
IV. WANNACRY RANSOMWARE

In 2017, one of the most [3] devastating crypto-ransomware named WannaCry began to spread and infect over 230,000 computers in more than 140 countries within a day. It targeted computers running Windows as an operating system. It spread through a worm known as WannaCrypt, Wanna Decryptor 2.0, WannaCrypt0r 2.0 and Wanna Decryptor. This worm was capable of automatically spreading itself using a transport mechanism. This mechanism first scans for vulnerable systems, then uses the EternalBlue exploit to gain access and a tool called DoublePulsar to install and execute a copy of itself.

The Common Vulnerabilities and Exposures number of EternalBlue is logged in the National Vulnerability Database as CVE-2017-0144. EternalBlue was released by Shadow Brokers. It works by taking advantage of the present SMBv1 vulnerabilities by making use of the way Microsoft Windows mishandles specially crafted packets from attackers.

DoublePulsar was developed by the U. S. National Security Agency's (NSA) Equation Group and leaked by Shadow Brokers. It is a backdoor implant tool and played a massive role in the spread of WannaCry.

The program first attempts an HTTP connection to www . iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea . com. If it is able to access it, it shuts itself down, and researchers believe that the developers placed this in case they wanted to pull the plug.

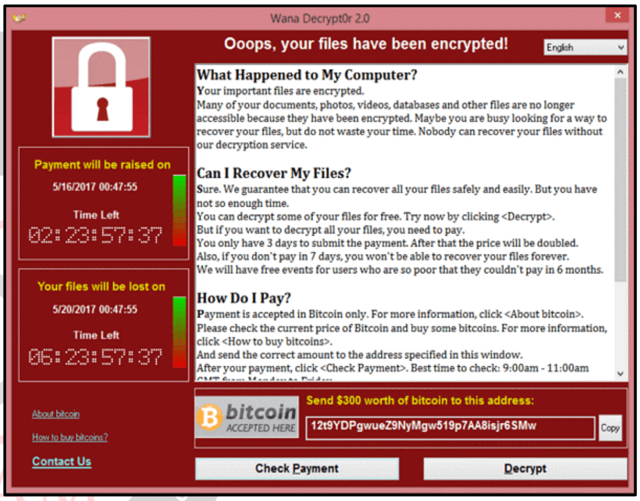


.der .pfx .key .crt .csr .p12 .pem .odt .ott .sxw .stw .uot .3ds .max .3dm .ods .ots
.sxc .stc .dif .slk .wb2 .odp .otp .sxd .std .uop .odg .otg .sxm .mml .lay .lay6 .asc
.sqlite3 .sqlitedb .sql .accdb .mdb .dbf .odb .frm .myd .myi .ibd .mdf .ldf .sln .suo
.cpp .pas .asm .cmd .bat .ps1 .vbs .dip .dch .sch .brd .jsp .php .asp .java .jar
.class .mp3 .wav .swf .fla .wmv .mpg .vob .mpeg .asf .avi .mov .mp4 .3gp .mkv .3g2
.flv .wma .mid .m3u .m4u .djvu .svg .psd .nef .tiff .tif .cgm .raw .gif .png .bmp .jpg
.jpeg .vcd .iso .backup .zip .rar .tgz .tar .bak .tbk .bz2 .PAQ .ARC .aes .gpg .vmx
.vmdk .vdi .sldm .sldx .sti .sxi .602 .hwp .snt .onetoc2 .dwg .pdf .wk1 .wks .123 .rtf
.csv .txt .vsdx .vsd .edb .eml .msg .ost .pst .potm .potx .ppam .ppsx .ppsm .pps .pot
.pptm .pptx .ppt .xltm .xltx .xlc .xlm .xlt .xlw .xlsb .xlsm .xlsx .xls .dotx .dotm
.dot .docm .docb .docx .doc

Fig.1 Targeted Extensions

After infection, it enumerates all the available disks. It targets files with particular extensions which are linked with database applications, multimedia formats, compressed archives and productivity. The following extensions mentioned in Fig.1 were targeted.WannaCry skips the files whose path names contain specific whitelisted directory names and language lists.

The encryption uses a combination of RSA and AES algorithms to encrypt files. WannaCry generates a private RSA-2048 key pair, encrypts this key with an embedded RSA public key, and stores it on a local disk with a .eky extension. This RSA key is used to encrypt the AES-128 key that is created randomly for each encrypted file. Each targeted file is opened, read, encrypted in memory, and then written to a new file with the filename format <random number>.WNCRYT in the malware's working directory. After that, the files are renamed to their original names, followed by the. WINCRY extension, and are sent to their original directory.



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

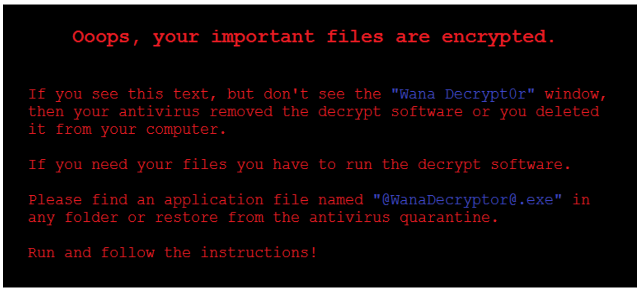
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Fig .2 Interface of Ransomware

Following the encryption of the file system, a window opens with the ransom demand interface. This window is continuously monitored by the malware. It reopens the window if it is closed. A program named taskse.exe checks active RDP sessions and displays the window shown in Figure 2 to the remote user as well.

The desktop wallpaper is also changed to the image shown in Fig. 3.



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

Fig.3 WannaCry Infected Wallpaper

DOI : 10.35291/2454-9150.2022.0008

This window demands the ransom, giving the victim hope to get his data back. It displays a counter from the time of infection and demands payment of USD300$ in bitcoin within three days. If this payment is not made these days, it increases to USD600$. Further, if the payment is still not paid within 7 days of the infection, the files will be permanently unrecoverable. The payment is required to be made at one of three hardcoded bitcoin wallet addresses.

Marcus Hutchins, a UK based researcher, discovered the killswitch hardcoded in the malware. He registered a domain name for the DNS sinkhole, which prevented the worm from spreading even further as the ransomware only encrypted files if it was unable to connect to that domain. This, however, did not help the already infected devices but helped slow down the spread to the other parts of the world.

Microsoft issued security bulletin MS17-010, which gave information about the EternalBlue flaw and announced patches released for all Windows versions that were currently supported at that time, these being Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.

V. Effects Of Ransomware

Ransomware causes a huge impact [4] on a company. It can lead to the temporary or permanent loss of the company's data, cause a temporary shutdown of the company and can result in a large financial loss of the company, which tarnishes the reputation of the company.

Ransomware assaults have grown all too regular in recent years. According to Fortinet, the average weekly ransomware activity was 10.7 times greater in June 2021 than the previous year. Demands from cybercriminals are likewise increasing: According to Coveware, the average ransom payment in the first quarter of 2021 was $220,298, up 43 percent from the fourth quarter of 2020.

According to the Ponemon Institute and Proofpoint, in addition to the ransom, business disruptions result in a maximum loss of $67.5 million during a ransomware infestation. According to Keeper Security's 2021 Ransomware Impact Report, 77 percent of full-time employees temporarily lost access to networks or systems when ransomware hit their firm, and 26 percent couldn't fully execute their professional obligations for at least a week.

Loss in productivity is a major driver of overall ransomware-related costs. A big factor to consider is the huge amount of resources and labor required to resolve the problem. An assessment is needed to understand if the organization has enough resources to determine what a ransomware incident could mean in terms of emergency consulting fees. For example, in one ransomware incident response engagement during the first five days of the incident, eleven of the all the team members had to put in thirty hours of overtime work to handle the situation. Over the course of 60 days, a dozen of the team members had worked over 1000 hours to contain and solve the issue so as to restore the IT business operation all of which had cost a huge amount for the organization. Completely mediating a ransomware attack takes an average of 32000 hours, according to the Ponemon Institute and Proofpoint.

Although the origin place where ransomware started was allegedly Russia and Eastern Europe, ransomware attacks are now common in almost all the countries, and The United States is now the top targeted nation for Ransomware Attacks.

There are 30-40 publicly named companies among the likely thousands that were impacted by Wannacry Ransomware. Examples include the Russian Interior Ministry, Telefonica (Spain's largest TeleCom Company) and FedEx. The UK National Health Service was severely hit with 16 of the 47 NHS trusts being affected and many of the operations, such as doctor appointments, being canceled.

There were reports that in China in 2016, over 40,000 organizations were affected, including 60 academic institutions. The figure below shows the countries affected by Ransomware in 2016.

Companies understand the dangers that ransomware poses and that attacks are inevitable. If the ransomware is not detected in time critical business related data could be encrypted causing a lot of disruptions to the business operations. Once a company has received a ransom demand it's too late to protect the system. Most of the companies that are attacked or demanded to pay a ransom do not admit to being attacked to protect their company's value.

There are several reasons why a company would pay the demanded ransom. Firstly paying the ransom restores the data that had been locked by the attackers. This causes a lot of problems to the company and in order to get all the operations of the company back to normal. Paying a ransom is a business decision. If the cost to recover from the ransomware attack exceeds the ransom payment then the company obviously opt for paying the ransom. Besides the business data there is sensitive customer and employee data that if leaked could cause a huge loss to the company business.

A lot of company's pay the demanded ransom but federal agencies and industry analysts agree that paying ransom does more than not paying it. While paying up the ransom seems a viable way to solve the problem, there are several reasons why companies should not pay the demanded ransom to the attackers. Paying the ransom encourages the hackers to run future attacks on more reputed companies. With the attacks increasing the attackers ask for 2 payments. First which is made for the decryption key and second payment for ensuring that the data is not released. Even if the company pays up the ransom it's completely up to the attackers,

DOI : 10.35291/2454-9150.2022.0008

whether they want to decrypt the data or ask for a bigger ransom. Paying up the ransom can also cause legal issues since it can be viewed as funding acts of terrorism depending upon the country the hacker group is operating out of. The biggest problem about paying the ransom is that it encourages new attackers which ask for a larger sum of money.

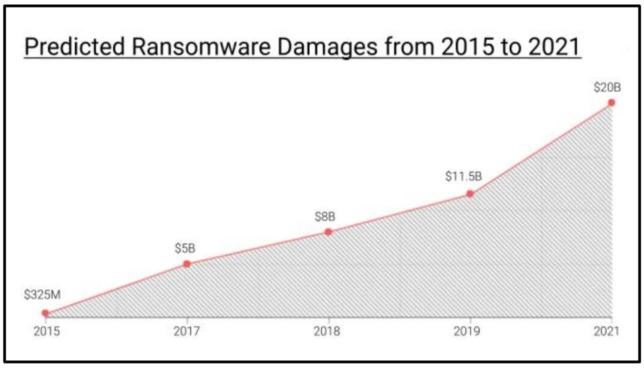


Fig. 4 Predicted Ransomware damages in USD($)

The graph in Fig. 4 [10] shown in Figure 4 indicates the increasing amount of damages sustained by major companies in USD through ransomware attacks per year according to [5] SecurityBoulevard. The increasing amount of damages suggests increasing interest in Ransomware attacks by attackers and only highlights this issue on a broader scale. This graph also indicates that the attackers are being encouraged to attack bigger companies and demand bigger ransoms.

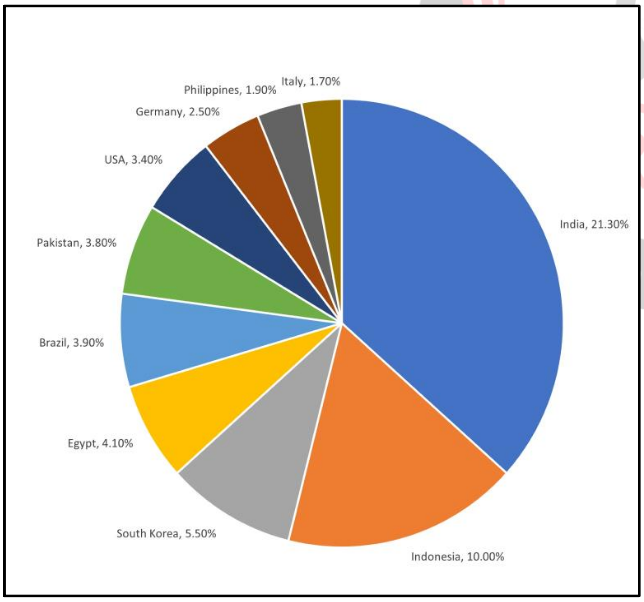


Fig. 5 Ransomware submissions by countries

The pie chart in Fig. 5 shows [9] the ransomware submissions made by different countries. According to the pie chart India has paid the highest amount of ransom in the past 10 years followed by Indonesia. Third world countries that are not thoroughly aware about Ransomware attacks end up paying the ransom and are the worst affected by it. Countries like The US counter ransomware attacks by contacting the Cyber Security experts and try to track down their attackers to save their money.

VI. Precautions and Preventive Measures

Avoid Suspicious Links

Emails, [6] messages, or websites can lead you to scripts which may attempt to load malware onto your system without you realizing. Avoiding certain links can reduce the susceptibility of a ransomware infection.

Ignore Scareware

Scareware is a message indicating your information has been 'hacked' or 'stolen' either demanding payment or recommending you install a fixer program to solve the issue. The program installed *is* the malware, relying on the user to make a snap decision.

Backup Files

Having a backup of all your files on a daily basis can help the user in case of a ransomware infection.

Antivirus and Firewalls

Having both firewalls and anti-virus running reduces the chances of ransomware infections. This will also inform you of any potential threats, flag suspicious activity, and overall act as an initial safeguard.

Use VPN and Encrypted Connections

The user can also use a virtual private network to encrypt your connection when browsing the web. This is also useful for travel when you use public wi-fi or other unsecured networks. Ransomware attacks rely on stealing login data or other personal info, so encryption is a useful way to prevent this.

Install Script Blockers

Adding script blocking add-ons to your browser are useful ways to prevent ransomware attacks, along with other malicious activity. A script-blocker can work with virtually any browser and gives the user direct control of what runs on a website.

Conduct Stress Tests

As a business, stress testing the cybersecurity infrastructure with drills to see how effective the defenses are is a good practice. You can also simulate what your business does in the event of a successful attack. This would give a good idea in case of a successful ransomware infection.

VII. Conclusion

Ransomware attacks are on the rise and are only going to keep increasing in the future. Targeted [8] ransomware is not confined to one specific industry. It has affected everything from healthcare organizations to sports and fitness companies. Organizations are constantly being targeted by attackers in an attempt for financial gain. With the increase

DOI : 10.35291/2454-9150.2022.0008

in data being digitally stored, the threat of ransomware gets even greater.

Every organization needs to have robust security measures in place to protect themselves against these attacks. They should ensure that all the software they use is patched to the latest versions. Backups should be created and stored in a location that is not connected to the network to prevent them from getting attacked as well.The employees of the organization should be trained to be well-versed with phishing attacks to avoid opening any suspicious links and thus giving the attackers an opportunity to infect the network.

WannaCry is just one of the many major ransomware attacks and we might not be as lucky to find a killswitch in them as we did for WannaCry. The question of whether to pay the ransom or not is a tricky one as there is no guarantee of getting your data back.

The world is moving into a new area of ransomware, one aimed at the extortion of confidential information and extracting large amounts of money. Companies large and small need to think about comprehensive security measures to ensure the secure working of their organizations. If organizations themselves are not able to protect themselves, then it is going to be a bigger task for individuals. The attackers are usually from countries that have weak or non-existent law enforcement. Hence, it is evident that law enforcements are not going to slow down this wave of ransomware.

VIII. REFERENCES

[1]https://www.researchgate.net/publication/306048005_Experimental_Analysis_of_Ransomware_on_Windows_and_Android_Platforms_Evolution_and_Characterization

[2]http://troindia.in/journal/ijcesr/vol4iss10part4/103-106.pdf

[3]https://www.varonis.com/blog/ransomware-statistics-2021/

[4]https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/

[5]https://www.securityboulevard.com/

[6]https://www.executech.com/insights/how-to-protect-from-ransomware-10-precautions-to-take/

[7]https://www.csoonline.com/article/3236183

[8]https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/

[9]https://www.emsisoft.com/

[10]https://blog.malwarebytes.com/cybercrime/2019/05/microsoft-pushes-patch-to-prevent-wannacry-level-vulnerability/

DOI : 10.35291/2454-9150.2022.0008